UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/751,899	12/27/2000	David W. Grawrock	42390P9844	9094

8791 7590 06/02/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
MAHMOUDI, HASSAN	

ART UNIT	PAPER NUMBER
2165	

DATE MAILED: 06/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/751,899	**Applicant(s)** GRAWROCK, DAVID W.	
	Examiner Tony Mahmoudi	**Art Unit** 2165	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _27 April 2005_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-21_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-21_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

SAM RIMELL
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's Request for Continued Examination (RCE) and amendments filed on 27-April-2005 has been entered.

Remarks

2. In response to communications filed on 27-April-2005, claims 12, 15 and 19 are amended per applicant's request. Claims 1-21 are presently pending in the application, of which, claims 1, 12, 15 and 19 are presented in independent form.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rallis et al (U.S. Patent No. 6,6,425,084) in view of Adams et al (U.S. Patent No. 6,363,485.)

As to claim 1, Rallis et al teaches a method comprising:

authenticating a user of a platform during a Basic Input/Output System (BIOS) boot process (see column 3, lines 14-17);

releasing a first keying material from a token communicatively coupled to the platform in response to authenticating the user (see column 3, lines 18-29 and see column 5, lines 9-21); and

decrypt a second BIOS area to recover a second segment of BIOS code (see column 1, line 67 through column 2, line 2 and see column 4, lines 10-11, where "decrypting" of "validation records" is taught, and see column 3, lines 14-17, where the "validation program" resides in "a ROM adapter 34 of the BIOS 30 and is executed at boot-up".)

Rallis et al does not teach:

combining the first keying material with a second keying material internally stored within the platform in order to produce a combination key; and

using the combination key to decrypt code.

Adams et al teaches a multi-factor biometric authentication device and method (see Abstract), in which he teaches combining the first keying material with a second keying material internally stored within the platform in order to produce a combination key (see Abstract, and see column 2, lines 34-39, and see column 3, lines 10-17); and using the combination key to decrypt code (see column 2, lines 48-62, and see column 5, lines 44-54, where the "combination key" is read on "secret key".)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rallis et al to include combining the first keying material with a second keying material internally stored within the platform in order to produce a combination key; and using the combination key to decrypt code.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rallis et al by the teaching of Adams et al, because combining the first keying material with a second keying material internally stored within the platform in order to produce a combination key; and using the combination key to decrypt code, would provide more security for user authentications than using a single key for decryption.

As to claim 2, Rallis et al as modified, teaches the method further comprising: continuing the BIOS boot process (see Rallis et al, column 3, lines 6-13.)

As to claims 3 and 13, Rallis et al as modified, teaches wherein prior to authenticating the user (see Rallis et al, column 3, lines 14-17), the method comprises:

loading a BIOS code including a first BIOS area and a second BIOS area (see Rallis et al, column 3, lines 6-13, where "loading" is read on "reading into the main RAM"), the first BIOS area being an encrypted first segment of the BIOS code and the second BIOS area being an encrypted second segment of the BIOS code (see Rallis et al, column 4, lines 10-11, where "decrypting portions" of the validation record is taught.)

As to claims 4, 14 and 16, Rallis et al as modified, teaches wherein after loading of the BIOS code (see Rallis et al, column 3, lines 6-13, where "loading" is read on "reading into the main RAM"), the method further comprises:

decrypting the first BIOS area to recover the first segment of the BIOS code (see Rallis et al, column 4, lines 10-11.)

As to claim 5, Rallis et al as modified, teaches the method further comprising:

unbinding keying material associated with a non-volatile storage device to access contents stored within the non-volatile storage device (see Rallis et al, column 4, lines 27-34, where 'unbinding keying material to allow accessing contents" is read on "commencing normal computer operations".)

As to claim 6, Rallis as modified teaches wherein the combination key is a value formed by performing an exclusive OR operation on both the first keying material and the second keying material (see Adams et al, Abstract, and see column 3, line 59 through column 4, line 3.)

As to claim 7, Rallis et al as modified, teaches wherein authentication of the user is performed through biometrics (see Rallis et al, column 5, lines 9-21, where "biometrics" is read on "finger print reader", and see Adams et al, column 2, lines 31-47.)

As to claim 8, Rallis et al as modified, teaches wherein the second keying material is stored within internal memory of a trusted platform module (see Adams et al, column 4, line 66 through column 5, line 1.)

As to claim 9, Rallis et al as modified, teaches wherein the second keying material is stored within a section of access-controlled system memory of the platform (see Adams et al, column 5, lines 55-64.)

As to claim 10, Rallis et al as modified, teaches wherein prior to authenticating the user, the method comprises:

loading a BIOS code including a first BIOS area being a first segment of the BIOS code encrypted using a selected keying material (see Rallis et al, column 3, lines 6-13, where "loading" is read on "reading into the main RAM"); and

loading an integrity metric including a hash value of an identification information of the platform (see Adams et al, figure 5 and see column 4, line 60 through column 5, line 15.)

As to claim 11, Rallis et al as modified, teaches wherein the identification information includes a serial number of an integrated circuit device employed within the platform (see Rallis et al, Abstract, see column 1, lines 45-58.)

As to claim 12, Rallis et al teaches an integrated circuit device (see Abstract and see figure 2) comprising:

a boot block memory unit (see column 3, lines 4-16); and

a trusted platform module communicatively coupled to the boot block memory unit (see figures 1A and 1B and see column 1, line 45 through column 2, line 57), and to decrypt a second BIOS area to recover a second segment of BIOS code (see column 1, line 67 through column 2, line 2 and see column 4, lines 10-11, where "decrypting" of "validation records" is taught, and see column 3, lines 14-17, where the "validation program" resides in "a ROM adapter 34 of the BIOS 30 and is executed at boot-up".)

Rallis et al does not teach to produce a combination key by combining a first incoming keying material with a second keying material internally stored within the integrated circuit and using the combination key to recover a segment of BIOS code.

Adams et al teaches a multi-factor biometric authentication device and method (see Abstract), in which he teaches to produce a combination key by combining a first incoming keying material with a second keying material internally stored within the integrated circuit (see Abstract, and see column 2, lines 34-39, and see column 3, lines 10-17) and using the combination key to recover a segment of BIOS code (see column 2, lines 48-62, and see column 5, lines 44-54, where the "combination key" is read on "secret key".)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rallis et al to include producing a combination key by combining a first incoming keying material with a second keying material internally stored within the integrated circuit.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rallis et al by the teaching of Adams et al, because producing a combination key by combining a first incoming keying material with a second keying material internally stored within the integrated circuit and using the combination key to recover a segment of BIOS code, would provide more security for user authentications than using a single key for decryption.

As to claim 15, Rallis et al teaches a platform (see figures 1A and 1B) comprising:

an input/output control hub (ICH) (see column 2, lines 45-57);

a non-volatile memory unit coupled to the ICH (see figure 2), the non-volatile memory unit including a BIOS code (see column 3, lines 4-17.)

For the remaining steps of this claim, the applicant is kindly directed to remarks and discussions made in claims 12 and 13 above.

As to claim 17, Rallis et al as modified, teaches the platform further comprising a hard disk drive coupled to the ICH (see Rallis et al, figure 2.)

As to claims 18 and 21, Rallis et al as modified, teaches wherein the trusted platform module to further unbind keying material associated with the hard disk drive to access contents stored within the hard disk drive (see Rallis et al, column 4, lines 27-34, where 'unbinding keying material to allow accessing contents" is read on "commencing normal computer operations".)

As to claim 19, Rallis et al teaches a program loaded into readable memory for execution by a trusted platform module of a platform (see column 3, lines 6-13, where "loading" is read on "reading into the main RAM").

For the remaining steps of this claim, the applicant is kindly directed to remarks and discussions made in claims 12 and 15 above.

As to claim 20, Rallis et al as modified, teaches wherein the first BIOS area is the first segment of the BIOS code encrypted with a keying material (see Rallis et al, column 1, line 67 through column 2, line 2 and see column 4, lines 10-11, where "decrypting" of "validation records" is taught, and see column 3, lines 14-17, where the "validation program" resides in "a ROM adapter 34 of the BIOS 30 and is executed at boot-up) and the second BIOS area is the second segment of the BIOS code encrypted with the combination key (see Adams et al, column 2, lines 34-39 and lines 48-62, see column 3, lines 10-17, and see column 5, lines 44-54, where the "combination key" is read on "secret key".)

Response to Arguments

5. Applicant's arguments filed on 27-April-2005 with respect to the rejected claims in view of the cited references have been fully considered but they are moot in view of the new grounds for rejection.

Conclusion

6. Any inquiries concerning this communication or earlier communications from the examiner should be directed to Tony Mahmoudi whose telephone number is (571) 272-4078. The examiner can normally be reached on Mondays-Fridays from 08:00 am to 04:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici, can be reached at (571) 272-4083.

tm

May 25, 2005

SAM RIMELL
PRIMARY EXAMINER